NCPROTECT™

TECHNICAL SPECIFICATIONS

The following technical requirements represent the minimum recommended configuration for installing NC Protect version 8.7. archTIS recognizes that each deployment is different and can advise on how your specific environment should be configured to ensure optimal performance. For the complete list of requirements and details, please refer to the Product Installation Guide.

SOFTWARE REQUIREMENTS

For Microsoft 365 installations

- SharePoint Online
- Microsoft Azure Subscriptions (e.g. Pay-as-you-go)
- Azure Active Directory

For SharePoint on-premises installations

- Microsoft SharePoint® 2016, 2019, SE or greater
- 64-bit version of Microsoft SQL® Server 2012 and later
- Microsoft SQL Server 2012 Reporting Services or later (optional)
- Microsoft .NET® Framework 4.8 and later
- Microsoft Entra ID® Active Directory RMS or Azure® for Encryption
- Internet Information Server 8.5 and later

For standalone Windows Server installations

- Microsoft Windows Server 2012 and later
- Internet Information Server 8.5 and later
- Microsoft .NET Framework 4.8 and later
- 64-bit version of Microsoft SQL® Server 2012 and later
- Microsoft SQL Server 2012 Reporting Services or later (optional)
- File Share (WebDAV)
- Microsoft® URL Rewrite Module 2.0 for IIS
- Windows PowerShell 5.1
- Microsoft Entra ID® Active Directory RMS or Azure for Encryption

CLIENT BROWSER

- Microsoft Edge (latest publicly released version)
- Google Chrome® (latest publicly released version)
- Mozilla Firefox® (latest publicly released version)
- Apple Safari (latest publicly released version)

AZURE REQUIREMENTS

For Microsoft 365 installations

- Azure app service, Azure SQL and Azure Storage resources and scale up capability should be configured as appropriate for client use case.

HARDWARE REQUIREMENTS

For on-premises installations

- 64-bit, four or eight core CPU (depending on the deployment size)
- At least 16GB RAM

QUESTIONS?

For more information on the required technical specifications, or to discuss your specific enterprise requirements, please contact our Customer Support.

Customer Help Center including Knowledgebase and Ticketing Portal: https://help.archtis.com/ (login required)
No Help Center Account? Submit a ticket at: https://www.archtis.com/support/ | **Email:** support@archtis.com

CAPABILITIES

Classification

Apply metadata classification to files and items. Supports multi-label classification.

Alternatively use or augment existing classifications from Microsoft Purview Information Protection (MPIP) labels, Janusnet Janusseal Documents, Titus, etc.

Default document types that can be classified/tagged using NC Protect: .TXT, .CSV, .DOC, .DOCX, .XLS, .XLSX, .PPT, .PPTX, .PDF*, .ASPX, .HTM, .HTML, CAD (.dgn, .dwf, .dwfx, .dwg, .dwt, .dxf, .ifc, .iges, .plt, .stl, .cff2), .png, .jpg, .jpeg, .tif, .tiff, .bmp, list items and events such as calendar entries.

Encryption Out-of-the-Box

Encrypt at rest or in transit of any file type supported natively by MPIP and additional file types with the appropriate Microsoft client install.

NC Encrypt Module (Optional)

The NC Encrypt add-on module enables encryption of files at rest in SharePoint Online and SharePoint Server via Bring Your Own Key (BYOK) using built-in key generation that uses AES-256 bit encryption that is FIPS140-2 compatible and provides remote key management for M365. It also supports integration with Thales CipherTrust Manager.

Secure Reader

Document types supported by the Secure Reader: .TXT, .CSV, .DOC, .DOCX, .XLS, .XLSX, .PPT, .PPTX, .PDF*, .ASPX, .HTM, .HTML, .EML, .MSG, CAD (.dgn, .dwf, .dwfx, .dwg, .dwt, .dxf, .ifc, .iges, .plt, .stl, .cff2), .png, .jpg, .jpeg, .tif, .tiff, .bmp, list items and events such as calendar entries.

Conditional Access & Usage Rights

NC Protect provides attribute-based augmentation of access and enforcement of usage rights for files, emails, and chat messages:

- Encrypt in-transit.
- Enforce read only access using a web-based file viewer.
- Apply dynamic watermarks and visual markings.
- Redact words and phrases.
- Control editing, copying, printing and download rights.

SUPPORTED PLATFORMS

Microsoft 365 & GCC High SharePoint Online

Classification, conditional access and usage, and encryption of SharePoint contents within list and libraries: Document library, Pages library, Generic list, Events list (calendar) and Tasks list.

SharePoint Server

Scanning, classification, conditional access and usage, and encryption of SharePoint contents within list and libraries: Document library, Pages library, Generic list, Events list (calendar) and Tasks list.

Microsoft 365 Exchange Online & Exchange Server

Classification and conditional access to attachments and encryption at rest of email messages (MSG).

Windows File Shares

Scanning, classification, conditional access and usage, and encryption of file types as above.

- The file system must be on a Microsoft Windows server and be in the same AD domain as the server where NC Protect is installed or in a trusted domain.

Nutanix® Files & NetApp® ONTAP®

Scanning, classification, conditional access and usage, and encryption of file types as above.

- The file system must be on a Nutanix Files or NetAPP ONTAP server and be in the same AD domain as the server where NC Protect is installed or in a trusted domain.

INTEGRATIONS / CONNECTORS

SIEM Applications

Ingest NC Protect's user activity and protection logs into Microsoft Sentinel or Splunk for further analysis and downstream actions to build additional insights from the data and cross-correlate it with your ecosystem, streamline investigation, automate responses, and more.

Janusseal Documents

The Janusseal Documents integration allows customers to use NC Protect's classification engine, leverage existing classifications, or a combination of the two, as part of the attributes used for enacting the product's dynamic ABAC policies.

Thales CipherTrust Manager

Connect directly to existing HSM/VSMs via integration with Thales CipherTrust Manager. The NC Encrypt CTM Connector provides an intuitive interface that enables you to leverage your existing CipherTrust Manager keys to encrypt Microsoft application content.